Amendments to the Claims

This listing of the claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Canceled)

2. (Currently Amended) [[A]]The method as claimed in claim 4, wherein the stored module configuration profile is held separately from the computing apparatus.

3. (Currently Amended) [[A]]The method as claimed in claim 4, wherein the stored module configuration profile is ~~stored such that it is~~ accessible only by a cryptographic authentication process.

4. (Currently Amended) A method of protecting from modification computer apparatus comprising a plurality of functional modules, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, the method comprising:

~~storing~~ the trusted device retrieving a module configuration profile of at least one module within the plurality of functional modules, wherein the module configuration profile comprises a public key corresponding to a public key of the at least one module; ~~the computer apparatus; and~~

the trusted device communicating with the at least one module by transmitting a first data to the at least one module;

the at least one module responding to the communication from the trusted device by transmitting a second data to the trusted device, wherein the second data comprises a signature generated with the private key;

the trusted device verifying authenticity of the signature with the public key; ~~checking the actual module configuration against the stored module configuration,~~ and

inhibiting function of the computer apparatus if the signature is not authentic. ~~actual module configuration does not satisfactorily match the stored module configuration.~~

5. (Currently Amended) [[A]]The method as claimed in claim 4, wherein the trusted device is adapted to communicate securely with the ~~stored~~ module configuration profile.

6. (Currently Amended) [[A]]The method as claimed in claim 5, wherein the stored module configuration profile is stored in a security token.

7. (Currently Amended) [[A]]The method as claimed in claim 6, wherein the security token is a smart card.

8. (Canceled)

9. (Currently Amended) [[A]]The method as claimed in claim 4, wherein [[a]]the ~~stored~~ module configuration profile is held by a remote module validation authority.

10. (Canceled)

11. (Currently Amended) [[A]]The method as claimed in claim 6, wherein another copy of [[a]]the ~~stored~~ module configuration profile is held by a remote module validation authority and the remote validation authority provides a service allowing a replacement security token to be provided if [[a]]the security token is lost or stolen.

12. (Canceled)

13. (Currently Amended) Computer apparatus as claimed in claim 14, wherein the ~~stored~~ module configuration profile is held separately from the computing apparatus and wherein the computer apparatus is adapted to obtain the ~~stored~~ module configuration profile by a cryptographic authentication process.

14. (Currently Amended) Computer apparatus adapted for protection against modification, the computer apparatus comprising:

a plurality of modules[[,]]; ~~one of said modules being~~

a trusted device adapted to respond to a user in a trusted manner[[,]];

wherein the trusted device is adapted to ~~compare a module configuration of the computer apparatus against a stored module configuration.~~ retrieve a module configuration profile of at least one module within the plurality of modules, wherein the module configuration profile comprises a public key corresponding to a private key of the at least one module;

wherein the trusted device is adapted to communicate with the at least one module by transmitting a first data to the at least one module and to receive a second data from the at least one module, wherein the second data comprises a signature generated with the private key; and

wherein the trusted device is adapted to verify authenticity of the signature with the public key and inhibit function of the computer apparatus if the signature is not authentic.

15-21. (Canceled)

22. (Currently Amended) A method of protecting from modification computer apparatus comprising a plurality of functional modules by monitoring the configuration of functional modules within the computer apparatus, the method comprising:

~~storing~~ retrieving a module configuration profile of at least one module within the plurality of functional modules, wherein the module configuration profile comprises a public key corresponding to a private key of the at least one module; ~~the computer apparatus on a security token removably attachable to the computer apparatus; and~~

~~checking the actual module configuration against the stored module configuration, and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration.~~

communicating with the at least one module by transmitting a first data to the at least one module;

the at least one module responding to the communication by transmitting a second data to the trusted device, wherein the second data comprises a signature generated with the private key;

verifying authenticity of the signature with the public key; and

inhibiting function of the computer apparatus if the signature is not authentic.

23. (Currently Amended) [[A]]The method as claimed in claim 22, wherein the ~~stored~~ module configuration profile is stored such that it is accessible only by a cryptographic authentication process.

24. (Currently Amended) [[A]]The method as claimed in claim 23, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner and the trusted device is adapted to ~~perform the step of checking the actual module configuration against the stored module configuration.~~ retrieve the module configuration profile of at least one module, communicate with the at least one module and verify authenticity of the signature.

25-26. (Canceled)

27. (Currently Amended) [[A]]The method as claimed in claim 22, wherein the ~~stored~~ module configuration profile is ~~also~~ held by a remote module validation authority.

28-29. (Canceled)

30. (New) A method of protecting from modification computer apparatus comprising a plurality of functional modules, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, the method comprising:

the trusted device retrieving a module profile of at least one module within the plurality of functional modules, wherein the module configuration profile comprises a public key;

the trusted device communicating with a security token by transmitting a first data to the security token;

the security token responding to the communication from the trusted device by transmitting a second data to the trusted device, wherein the second data comprises a signature generated with a private key;

the trusted device verifying authenticity of the signature with the public key; and

inhibiting function of the computer apparatus if the signature is not authentic.

31. (New) The method as claimed in claim 30, wherein the module profile is held separately from the computing apparatus.

32. (New) The method as claimed in claim 30, wherein the module profile is accessible only by a cryptographic authentication process.

33. (New) The method as claimed in claim 30, wherein the trusted device is adapted to communicate securely with the module profile.

34. (New) The method as claimed in claim 33, wherein the module profile is stored in the security token.

35. (New) The method as claimed in claim 34, wherein another copy of the module profile is held by a remote module validation authority and the remote validation authority provides a service allowing a replacement security token to be provided if the security token is lost or stolen.

36. (New) The method as claimed in claim 30, wherein the security token is a smart card.

37. (New) The method as claimed in claim 30, wherein the module profile is held by a remote module validation authority.

38. (New) Computer apparatus adapted for protection against modification, the computer apparatus comprising:

a plurality of modules;

a trusted device adapted to respond to a user in a trusted manner;

wherein the trusted device is adapted to retrieve a module configuration profile of at least one module within the plurality of modules, wherein the module configuration profile comprises a public key;

wherein the trusted device is adapted to communicate with a security token by transmitting a first data to the security token and receive a second data from the security token, wherein the second data comprises a signature generated with a private key; and

wherein the trusted device is adapted to verify authenticity of the signature with the public key and inhibiting function of the computer apparatus if the signature is not authentic.

39. (New) Computer apparatus as claimed in claim 38, wherein the module configuration profile is held separately from the computing apparatus and wherein the computer apparatus is adapted to obtain the module configuration profile by a cryptographic authentication process.

40. (New) A method of protecting from modification computer apparatus comprising a plurality of functional modules by monitoring the configuration of functional modules within the computer apparatus, the method comprising:

retrieving a module configuration profile of at least one module within the plurality of functional modules, wherein the module configuration profile comprises a public key;

communicating with a security token by transmitting a first data to the security token;

the security token responding to the communication by transmitting a second data to the trusted device, wherein the second data comprises a signature generated with a private key;

verifying authenticity of the signature with the public key; and

inhibiting function of the computer apparatus if the signature is not authentic.

41. (New) The method as claimed in claim 40, wherein the module configuration profile is stored such that it is accessible only by a cryptographic authentication process.

42. (New) The method as claimed in claim 41, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner and the trusted device is adapted to retrieve the module configuration profile of the at least one module, communicate with the at least one module and verify authenticity of the signature

43. (New) The method as claimed in claim 40, wherein the module configuration profile is held by a remote module validation authority.